Docket No.: P-218 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of :

Sung-Kyun PARK :

Serial No.: Unassigned : Group Art Unit: Unassigned

Filed: August 23, 2001 : Examiner: Unassigned

For: METHOD FOR PROCESSING ACCESS-REQUEST MESSAGE FOR PACKET SERVICE

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Assistant Commissioner of Patents
Washington, D. C. 20231

Sir:

At the time the above application was filed, priority was claimed based on the following application:

Republic of Korea Patent Application No. 50068/2000, filed August 28, 2000.

A copy of the priority application listed above is enclosed.

Respectfully submitted,
FLESHNER & KIM, LLP

Daniel Y.J. Kim
Registration No. 36,186
Anthony H. Nourse
Registration No. 46,121

P. O. Box 221200
Chantilly, Virginia 20153-1200
703 502-9440
Date: August 23, 2001
DYK:AHN/jad

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 50068 호
Application Number

출 원 년 월 일 : 2000년 08월 28일
Date of Application

출 원 인 : 엘지정보통신주식회사
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2001 년 01 월 05 일

특 허 청
COMMISSIONER

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2000.08.28
【발명의 명칭】	에이에이에이 서버에 과부하 방지를 위한 접근요청 메시지 처리 방법
【발명의 영문명칭】	Access-request messgae handling method for over load prevention at AAA server
【출원인】	
【명칭】	엘지정보통신 주식회사
【출원인코드】	1-1998-000286-1
【대리인】	
【성명】	김영철
【대리인코드】	9-1998-000040-3
【포괄위임등록번호】	1999-010680-1
【발명자】	
【성명의 국문표기】	박성균
【성명의 영문표기】	PARK,Sung Kyun
【주민등록번호】	690611-1037618
【우편번호】	121-210
【주소】	서울특별시 마포구 서교동 395-113
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 김영철 (인)
【수수료】	
【기본출원료】	16 면 29,000 원
【가산출원료】	0 면 0 원
【우선권주장료】	0 건 0 원
【심사청구료】	3 항 205,000 원
【합계】	234,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 해커들이 전송하는 일시적인 수많은 접근요청 메시지로 인한 AAA서버의 과부하를 방지하도록 접근요청 메시지에 대해 메시지의 속성을 분석하지 않고 메시지 자체로 처리하는 AAA서버에 과부하를 방지하기 위한 접근요청 메시지 처리 방법에 관한 것이다.

종래에는 해커가 다량의 접근요청 메시지를 AAA서버로 전송하면, 해당 AAA서버는 거짓의 접근요청 메시지에 대해서도 메시지 자체가 아니라 메시지 내부의 속성부까지 검증하여야 메시지를 판별 할 수 있고, 판별을 수행하는 데는 데이터베이스의 조회, 기타 자원의 할당 등 여러 처리 과정이 필요하여 AAA서버 시스템에 과부하가 걸리는 문제점이 있다.

따라서, 본 발명은 패킷 데이터 네트웍에서 해커들이 대량으로 전송하는 악의 적인 접근요청 메시지를 내부의 속성까지 분석하지 않고 메시지 자체만을 검증하여 잘못된 메시지를 처리하므로, AAA서버에 과부하가 발생하여 다운되는 현상을 방지하며, AAA서버 시스템의 자원과 시간 부하 등을 최대한 줄여 성능을 향상 시키고 자원을 절약하여 비용을 감소시키는 효과가 있다.

【대표도】

도 3

【명세서】

【발명의 명칭】

에이에이에이 서버에 과부하 방지를 위한 접근요청 메시지 처리 방법{Access-request messgae handling method for over load prevention at AAA server}

【도면의 간단한 설명】

도1은 종래의 FA와 AAA서버 사이에 메시지 흐름도.

도2는 종래의 RADIUS 프로토콜의 구성도.

도3은 본 발명에 따른 접근요청 메시지의 구성도.

* 도면의 주요 부분에 대한 부호의 설명 *

10 : FA(Foreign Agent), 12 : 접근요청(Access-Request),

11 : AAA(Authentication Authorization and Accounting),

13 : 접근허가(Access-Acept), 14 : 계정과금요청(Account-Request),

15 : 계정과금허가(Account-Response), 20, 30, 37 : 코드(Code),

21, 31, 38 : 식별자(Identifier), 22, 32, 39 : 길이(Length),

23 : 인증부(Authenticator), 24, 34~36, 41~43 : 속성부(Attribute),

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 AAA 서버에 관한 것으로, 특히 해커들이 전송하는 일시적인 수많은 접근

요청 메시지로 인한 AAA서버의 과부하를 방지하도록 접근요청 메시지에 대해 메시지의 속성을 분석하지 않고 메시지 자체로 처리하는 AAA서버에 과부하를 방지하기 위한 접근 요청 메시지 처리 방법에 관한 것이다.

<12> 일반적으로, AAA(Authentication, Authorization and Accounting)서버와 FA(Foreign Agent) 사이에 데이터의 송수신은 RADIUS(Remote Authentication Dial-In User Service) 프로토콜을 주로 사용한다. RADIUS는 원격접속 서버가 다이얼업(Dial-Up) 모뎀을 통하여 접속해온 사용자들을 인증하고, 요청된 시스템이나 서비스에 관해 접속자에게 접근권한(Authorization)을 부여하기 위한 중앙의 서버와 통신할 수 있게 해주는 클라이언트/서버 프로토콜이다. RADIUS 프로토콜은 중앙 데이터베이스 내에 사용자 정보를 유지하고, 모든 원격지 서버가 공유할 수 있게 한다. RADIUS 프로토콜에는 인증(Authentication), 권한부여(Authorization), 계정(Accounting) 메시지가 있다. 인증 메시지는 개별 또는 인터넷을 포함한 공공 네트웍에서의 로그온 시에 암호의 사용을 통하여 판단하며, 권한부여 메시지는 다중 사용자 컴퓨터 시스템에서 어떤 사용자가 해당 시스템을 액세스할 수 있는지, 파일의 접근 범위, 허용된 접근 시간, 할당된 저장 공간의 크기 등의 사용권한을 정의 하는 것이다. 계정 메시지는 사용자가 패킷 서비스를 개시했음과 얼마만큼의 패킷 서비스를 받았는지와, 패킷 서비스가 종료되었음을 알리기 위한 목적으로 사용한다.

<13> 종래에 무선단말기로 무선 패킷 데이터 서비스를 위하여 인터넷에 접속하는경우 패킷 데이터의 송수신을 담당하는 FA(Foreign Agent)와 AAA 서버 사이에는 RADIUS 프로토콜에 기반하여 메시지를 송수신한다. 인증, 권한부여, 계정 메시지에는 접근요청

(Access-Request), 접근허가(Access-Accept), 접근신청(Access-Challenge), 계정과금요청(Account-Request), 계정과금허가(Account-Response) 등의 메시지가 있다. 인증, 권한부여, 계정메시지들은 검증을 수행하기 위한 인증부를 보유하며, 접근요청 메시지의 경우 인증값(Authenticator)은 패킷 데이터 송수신을 담당하는 FA에서 임의로 발생시킨 것이다. 인증값은 중복이 되지 않으며, 바로 전에 사용했던 인증값을 다시 사용하지 않는다. 임의의 값으로 인증값을 사용하는 것은 해커가 메시지를 가로채서 악의적인 행동을 방지하기 위한 것이다. 인증값이 메시지에 관계없이 일정하다면 해커는 공유 비밀키를 모르더라도 해당 공유 비밀키를 기반으로 만들어진 메시지 내의 인증값을 이용하여 AAA 서버로부터 정상적인 접근허가를 얻을 수 있다. 따라서 인증값을 메시지의 송수신시 매번 변화시켜 해커로부터의 공격을 방어하는 것이다. 그리고, 접근요청 메시지 이외의 메시지의 인증값은 메시지 자체에 대한 알고리즘 수행 결과가 들어간다.

<14> 한편, 접근요청 메시지에는 인증값을 사용하여 사용자 비밀키를 암호화하여 AAA서버로 전송하며, 해당 AAA서버는 인증값을 사용하여 암호화된 사용자 비밀키를 해독하는 역할을 수행한다. 이런 이유로 인증값은 FA에서 사용자 비밀키를 암호화하기 이전에 생성된다. 따라서 접근요청 메시지는 주데이터의 속성부(Attribute)의 분석을 거쳐야 검증할 수 있다. 검증을 수행하는 데는 데이터베이스의 조회, 기타 자원의 할당 등 여러 처리 과정이 필요하여 AAA 서버 시스템에 과부하가 걸리는 문제점이 발생하며, 반면에 접근허가, 접근신청, 계정과금요청, 계정과금허가 메시지는 사용자 비밀키 부분이 없어서 인증값은 메시지 자체에 대한 검증을 하기 위해서만 사용된다. 만들어진 메시지 자체와 AAA 서버와 FA사이에 공유한 비밀키를 입력으로 MD5 알고리즘을 실행하여 인증값이 얻어진다. 접근허용, 접근선택, 계정과금요청, 계정과금허가 메시지들은 인증값이 메시지 자

체의 검증에 대해서 사용되므로, AAA 서버에서는 메시지를 수신하면 해당 메시지의 주데이터 속성인 내부 어트리뷰트에 대한 분석없이 MD5 알고리즘을 실행하여 메시지 자체를 검증하여 수용 또는 폐기할 수 있다.

<15> 도1을 참조하여 접근요청 메시지의 구성을 설명하면 다음과 같다. FA는 전체 패킷 데이터의 송수신을 담당하며, AAA 서버는 인증, 권한부여와 계정에 대한 과금 등의 기능을 수행한다. FA와 AAA 서버사이에는 RADIUS 프로토콜을 사용한다. RADIUS 프로토콜에서 메시지 송수신시에 데이터의 패킷 자체에 인증을 위하여 인증값을 사용하며 인증값은 예측할 수 없는 값으로 하여야 하며, 매 번 바뀌어야 하는 규정이 있다. 한편, 사용자가 무선 단말기로 무선 패킷 데이터 서비스를 요청하면 FA는 등록된 무선 단말기가 정상인지 여부를 확인하기 위한 절차로 접근요청 메시지를 사용하여 무선단말기에 대한 인증을 수행하고, 해당 AAA 서버는 RADIUS 프로토콜을 사용하여 무선단말기에 대한 인증을 수행한다. 한편, 패킷데이터 서비스를 설정에는 고정IP와 모바일IP 방식이 있으며, 고정IP의 인증에는 PAP(Password Authentication Protocol)방식과 CHAP(Challenge Handshake Authentication

Protocol) 방식이 있고, 패킷 데이터가 정상인지 여부를 인증값을 이용하여 검증을 수행한다. PAP방식은 PPP(Point to Point Protocol) 서버에 의해 사용되는 절차로 먼저 접속이 이루어 지면 사용자가 ID와 사용자 비밀키를 FA로 전송하고, FA가 ID와 사용자 비밀키를 확인하기 위해 사용자 비밀키를 암호화하여 AAA 서버로 접근요청 메시지를 보내어 그 결과에 따라 승인하거나 접속을 끊는 방식으로 사용자 비밀키는 FA까지는 보안절차 없이 전송되며, FA와 AAA 서버 사이에는 암호화되어 전송된다. 그리고, 사용자는 액세스 승인을 얻기 위해 반복적인 시도를 할 수 있다. CHAP 인증방식은 PAP보다 시스템에 안전하게 접속하기 위한 절차로 접속이 이루어 지면 서버가 사용자에게 확인 메시지를 전송하고 사용자가 단방향 해시함수를 이용하여 서버로 전송하며 서버는 해시값을 계산한 결과와 사용자가 응답한 값을 비교, 확인하여 두 값이 일치하면 인증이 승인되며, 그렇지 않으면 접속은 종료된다. CHAP 인증방식은 식별자들이 자주 변화하고 서버가 사용자에게 언제나 인증을 요청할 수 있기 때문에 PAP 인증 방식보다 더 안전하다. 모바일 IP 인증 방식은 고정 IP의 CHAP 인증방식과 같은 방식으로 인증된다. 또한, 인증과정을 마치면 AAA 서버는 무선단말기에 대한 접근허가 메시지를 FA로 송신하면 무선 패킷 데이터 서비스를 위한 설정은 끝나게 되어, 무선단말기와 FA사이에 패킷 데이터 송수신을 할 수 있게 되며, 해당 패킷 데이터 송수신이 시작되는 시점에 FA에서 과금을 위한 계정과금요청 메시지를 AAA서버로 전송한다. AAA 서버는 계정과금요청 메시지를 인증값을 근거로 검증하여 확인되면 계정과금허가 메시지를 FA로 전송하여 과금이 진행된다.

<16> 도2는 FA와 AAA 서버사이에 데이터 송수신에 쓰이는 RADIUS 프로토콜의 구조

이며 설명하면 다음과 같다. 코드(code)는 1 바이트로 메시지의 종류를 나타내며 식별자(Identifier)는 1byte로 여러 메시지를 구분하는 구분자이다. 길이(Length)는 전체 RADIUS 프로토콜 메시지의 길이부로 코드, 식별자, 길이 필드를 포함한 길이이다. 또한, 인증에 사용되는 인증값 16바이트가 있고 나머지 주 데이터의 속성을 나타내는 속성부가 RADIUS 프로토콜 메시지를 구성한다. FA와 AAA 서버 사이에 데이터 송수신에 사용되는 RADIUS 프로토콜의 메시지중에서 접근요청 메시지 이외의 모든 메시지들은 메시지 자체에 대한 검증을 수행하기 위해 인증값을 사용한다. 그래서 메시지 내부의 속성에 대한 분석없이 정상적인 메시지 여부를 판단할 수 있다. 그러나 접근요청 메시지는 해당 접근요청 메시지 내부의 주 데이터 속성에 대한 분석이 없이는 정상적인 메시지 여부를 구분할 수 없다. 이유는 메시지를 분석 없이 검증하기 위해서는 인증값을 메시지 자체를 기초로 하여 만들어져야 하는데 접근요청 메시지는 인증값을 이용하여 패킷 내부의 사용자 비밀키를 암호화하기 위해서 사용되기 때문에 나중에 만들어질 수 없기 때문이다. 나중에 만들어져야 AAA서버에서 메시지 자체와 공유 비밀키를 입력으로 MD5 알고리즘(암호화)을 수행해서 나온 값과 인증값과 비교할 수 있기 때문이다.

<17> 따라서, 종래의 RADIUS 프로토콜에서 사용하는 접근요청 메시지 처리 방식은 악의적인 해커가 다량의 거짓 접근요청 메시지를 AAA 서버로 보내게 된다면 AAA서버는 거짓 메시지에 대해서도 일일이 메시지 내부의 속성들을 분석하여 정상 메시지여부를 판별해야 하고, 판별의 수행을 위해 데이터베이스의 조회 및 자원 할당 등 여러가지 처리 과정이 들어가므로 AAA서버 시스템에 부하가 올라가는 과부화 현상을 초래하는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<18> 본 발명은 상술한 바와 같은 문제점을 해결하기 위한 것으로 그 목적은, 악의적인 해커에 의해 다량의 접근요청 메시지가 일시적으로 AAA서버로 전송되어도 AAA서버는 거짓의 접근요청 메시지에 대해서 메시지 자체만 검증하여 거짓의 접근요청 메시지를 적은 시간과 자원으로 판별 할 수 있도록 하여 AAA서버 시스템에 과부하를 방지하여 성능을 향상 시키고 자원을 절약하여 비용을 감소시키도록 하는데 있다.

【발명의 구성 및 작용】

<19> 상술한 바와 같은 목적을 달성하기 위한 본 발명의 특징은, FA(Foreign Agent)에서 인증부와 속성부를 포함하는 접근요청 메시지에서 임의의 인증값을 상기 속성부로 입력하는 과정과; 상기 속성부에 입력된 인증값으로 사용자 비밀키를 암호화하는 과정과; 상기 임의의 값으로 채운 인증부와 상기 속성부를 입력값으로 암호화 알고리즘을 실행하여 생성되는 메시지 다이제스트를 다시 인증부로 입력하는 과정과; 상기 인증부와 상기 속성부를 합친 접근요청 메시지를 AAA(Authentication Authorization and Accounting)서버로 전송하는 과정과; 상기 AAA서버에서 상기 접근요청 메시지를 검증하는 과정을 포함하는 에이에이에이 서버에 과부하 방지를 위한 접근요청 메시지 처리 방법을 제공하는데 있다.

<20> 그리고, 상기 AAA서버에서 접근요청 메시지를 검증하는 과정은, 상기 접근요청 메시지의 인증부에 저장되어 있는 상기 메시지 다이제스트를 별도로 저장하는 단계와; 상기 인증부에 임의의 값을 채운후, 해당 인증부와 속성부의 값을 입력으로 암호화 알고리

즘을 실행하여 출력인 인증값을 구하는 단계와; 상기 인증값과 상기 저장한 메시지 다이제스트를 비교하여 일치하면 정상사용자로 판단하는 단계를 포함하는 것을 특징으로 한다.

<21> 이때, 상기 접근요청 메시지는, 메시지 내부를 분석하지 않고 상기 인증값만으로 검증하는 것을 특징으로 한다.

<22> 이하, 본 발명에 따른 실시예를 첨부한 도면을 참조하여 상세하게 설명하면 다음과 같다. FA와 AAA서버 사이에 사용하는 RADIUS 프로토콜의 규칙에는 접근요청 메시지에 대한 인증값은 똑같은 내용의 속성을 가진 메시지라도 매 번 바뀌어야 하며, 같은 사용자 비밀키의 암호화에도 매 번 다른 결과가 나와야 한다. 즉, 인증값은 중복이 되지 않으며, 바로 전에 사용했던 인증값을 다시 사용하지 않는다. 임의의 값으로 인증값을 사용하는 것은 해커가 메시지를 가로채서 악의적인 행동을 방지하기 위한 것이다.

<23> 도3은 본 발명에 따른 접근요청 메시지를 구성하는 과정을 도시한 도면으로, 이를 상세하게 설명하면 다음과 같다. 코드(code)(30, 37)는 1 바이트로 메시지의 종류를 나타내며 식별자(Identifier)(31, 38)는 1byte로 여러 메시지를 구분하는 구분자이다. 길이(Length)(32, 39)는 전체 RADIUS 프로토콜 메시지의 길이부로 코드, 식별자, 길이 필드를 포함한 길이이다. 또한, 인증에 사용되는 인증값 16바이트가 있고 나머지 주 데이터의 속성을 나타내는 속성부가 RADIUS 프로토콜 메시지를 구성한다.

<24> 종래에는 접근요청 메시지 이외의 모든 메시지들은 메시지 자체에 대한 검증을 수행하기 위해 인증값을 사용한다. 그래서 메시지 내부의 속성에 대한 분석없이 정상적인

메시지 여부를 판단할 수 있다. 그러나 접근요청 메시지는 내부의 주 데이터 속성에 대한 분석이 없이는 정상적인 메시지 여부를 구분할 수 없어서 해커가 보내는 악의적인 접근요청 메시지를 처리하기 위해 AAA서버는 해당 접근요청 메시지의 주데이터의 속성을 분석하는데 과부하가 걸리는 문제점이 있었다.

<25> 한편, 본 발명에 따른 새로운 접근요청 메시지 처리 방법은 다음과 같다. FA에서 접근요청 메시지를 만드는 것은 PAP 인증방식의 경우, 먼저 임의의 인증값을 사용하지만 해당 인증값을 인증부(33)로 넣지않고 PASSWD_AUTH 속성부(35~36)의 값으로 입력한다. 해당 속성부(35~36)의 PASSWD_AUTH에 저장된 인증값으로 사용자 비밀키의 암호화를 수행하고, 접근요청 메시지의 형태(type), 길이(length), 값(value)등으로 속성부들도 만든다. 코드(30)에는 접근요청 메시지를 의미하는 1을 할당하고, 식별자(31)를 할당하며, 길이(32)를 넣는다. 인증부(33)에는 모두 0으로 채운 후 FA와 AAA 서버 사이에 공유 비밀키를 입력하여 MD5 알고리즘(암호화)을 실행한다. MD5 알고리즘을 실행한 결과 값인 16byte의 메시지 다이제스트(Message Digest) 즉, 인증값을 새로운 접근요청 메시지의 인증부(40)에 입력하고, 속성부(41~43)를 포함한 접근요청 메시지를 AAA서버로 송신한다. AAA 서버는 수신한 접근요청 메시지에서 인증부(40)의 인증값은 별도로 저장하고, 검증을 위해서 인증부(40)에 모두 0을 채운 후 FA와 AAA 사이에 공유하는 공유 비밀키를 입력으로 하여 MD5 알고리즘을 실행하면 16바이트의 메시지 다이제스트 값인 인증값이 출력된다. 검증으로 수신하여 별도로 저장한 인증값과 비교하여 같으면 정상적인 메시지로 판단하고 다르면 비정상적인 메시지로 판단한다. 따라서 거짓의 접근요청 메시지에 대해 메시지 내부의 속성부까지 검증하는데 필요한 데이터 베이스의 조회, 기타 자원의 할당 등의 여러 처리 과정이 줄어들게 된다.

<26> 한편, CHAP 인증 방식을 사용하는 경우에는 임의의 인증값을 인증부(33)로 넣지않고 CHAP_CHALLENGE라는 속성부(34~36)의 값으로 넣는다. 해당 속성부(34~36)의 CHAP_CHALLENGE에 저장된 인증값으로 사용자 비밀키의 암호화를 수행하고, 접근요청 메시지의 속성들도 만들어 코드(30)에는 접근요청 메시지를 의미하는 1을 할당하고, 식별자(31)를 할당하며, 길이(32)를 넣는다. 인증부(33)에는 모두 0으로 채운 후 FA와 AAA 서버 사이에 공유 비밀키를 입력하여 MD5 알고리즘을 실행한다. MD5 알고리즘을 실행한 결과 값인 16byte의 메시지 다이제스트 즉, 인증값 새로운 접근요청 메시지의 인증부(40)에 입력하고, 속성부(41~43)를 포함한 접근요청 메시지를 AAA서버로 송신한다. AAA 서버는 수신한 접근요청 메시지에서 인증부(40)의 인증값은 별도로 저장하고, 검증을 위해서 인증부(40)에 모두 0을 채운 후 FA와 AAA 사이에 공유하는 공유 비밀키와 메시지를 입력으로 하여 MD5 알고리즘을 실행하면 16바이트의 메시지 다이제스트 값인 인증값이 출력된다. 수신하여 별도로 저장한 인증값과 비교하여 같으면 정상적인 메시지로 판단하고 다르면 비정상적인 메시지로 판단한다. 또한, 모바일 IP 인증은 고정 IP의 CHAP 인증과 동일한 방식으로 인증된다.

<27> 상술한 바와 같이 다량의 접근요청 메시지에 대해 메시지 내부의 속성부까지 검증할 필요가 없어져서 데이터 베이스의 조회, 기타 자원의 할당 등의 여러 처리 과정이 줄어들게 되며, 고정 IP방식에서의 인증방식인 PAP와 CHAP에 적용할 수 있으며 모바일 IP방식에도 모두 적용하여 사용할 수 있다.

<28> 또한, 본 발명에 따른 실시예는 상술한 것으로 한정하지 않고, 본 발명과 관련하여 통상의 지식을 가진 자라면 자명한 범위 내에서 본 발명을 여러 가지로 수정 및 변경하여 실시할 수 있을 것이며, 이와같은 수정 및 변경은 본 발명의 기술적 범주에 해당함을

밝혀둔다.

【발명의 효과】

<29> 이상과 같이, 본 발명은 패킷데이터 네트웍에서 해커들이 다량으로 전송하는 일시적인 접근요청 메시지를 내부의 속성까지 분석하지 않고 메시지 자체를 검증하여 잘못된 메시지를 처리하므로, AAA 서버에 과부하가 발생하여 다운되는 현상을 방지하며, AAA 서버시스템의 자원과 시간 부하 등을 최대한 줄여 성능을 향상 시키고 자원을 절약하는 효과가 있다.

【특허청구범위】

【청구항 1】

FA(Foreign Agent)에서 인증부와 속성부를 포함하는 접근요청 메시지에서 임의의 인증값을 상기 속성부로 입력하는 과정과;

상기 속성부에 입력된 인증값으로 사용자 비밀키를 암호화하는 과정과;

상기 임의의 값으로 채운 인증부와 상기 속성부를 입력값으로 암호화 알고리즘을 실행하여 생성되는 메시지 다이제스트를 다시 인증부로 입력하는 과정과;

상기 인증부와 상기 속성부를 합친 접근요청 메시지를 AAA(Authentication Authorization and Accounting)서버로 전송하는 과정과;

상기 AAA서버에서 상기 접근요청 메시지를 검증하는 과정을 포함하는 것을 특징으로 하는 에이에이에이 서버에 과부하 방지를 위한 접근요청 메시지 처리 방법.

【청구항 2】

제1항에 있어서,

상기 AAA서버에서 접근요청 메시지를 검증하는 과정은, 상기 접근요청 메시지의 인증부에 저장되어 있는 상기 메시지 다이제스트를 별도로 저장하는 단계와;

상기 인증부에 임의의 값을 채운후, 해당 인증부와 속성부의 값을 입력으로 암호화 알고리즘을 실행하여 출력인 인증값을 구하는 단계와;

상기 인증값과 상기 저장한 메시지 다이제스트를 비교하여 일치하면 정상사용자로 판단하는 단계를 포함하는 것을 특징으로 하는 에이에이에이 서버에 과부하 방지를 위한

접근요청 메시지 처리 방법.

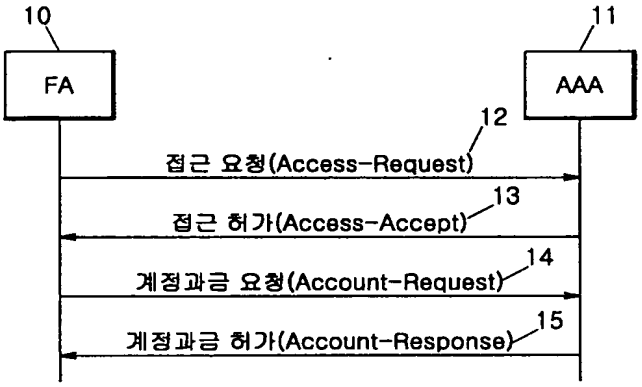
【청구항 3】

제1항 또는 2항에 있어서,

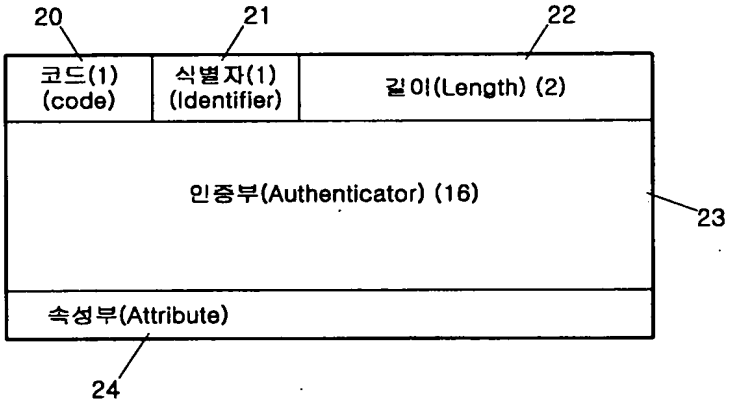
상기 접근요청 메시지는, 메시지 내부를 분석하지 않고 상기 인증값만으로 검증하는 것을 특징으로 하는 에이에이이에이 서버에 과부하 방지를 위한 접근요청 메시지 처리 방법.

【도면】

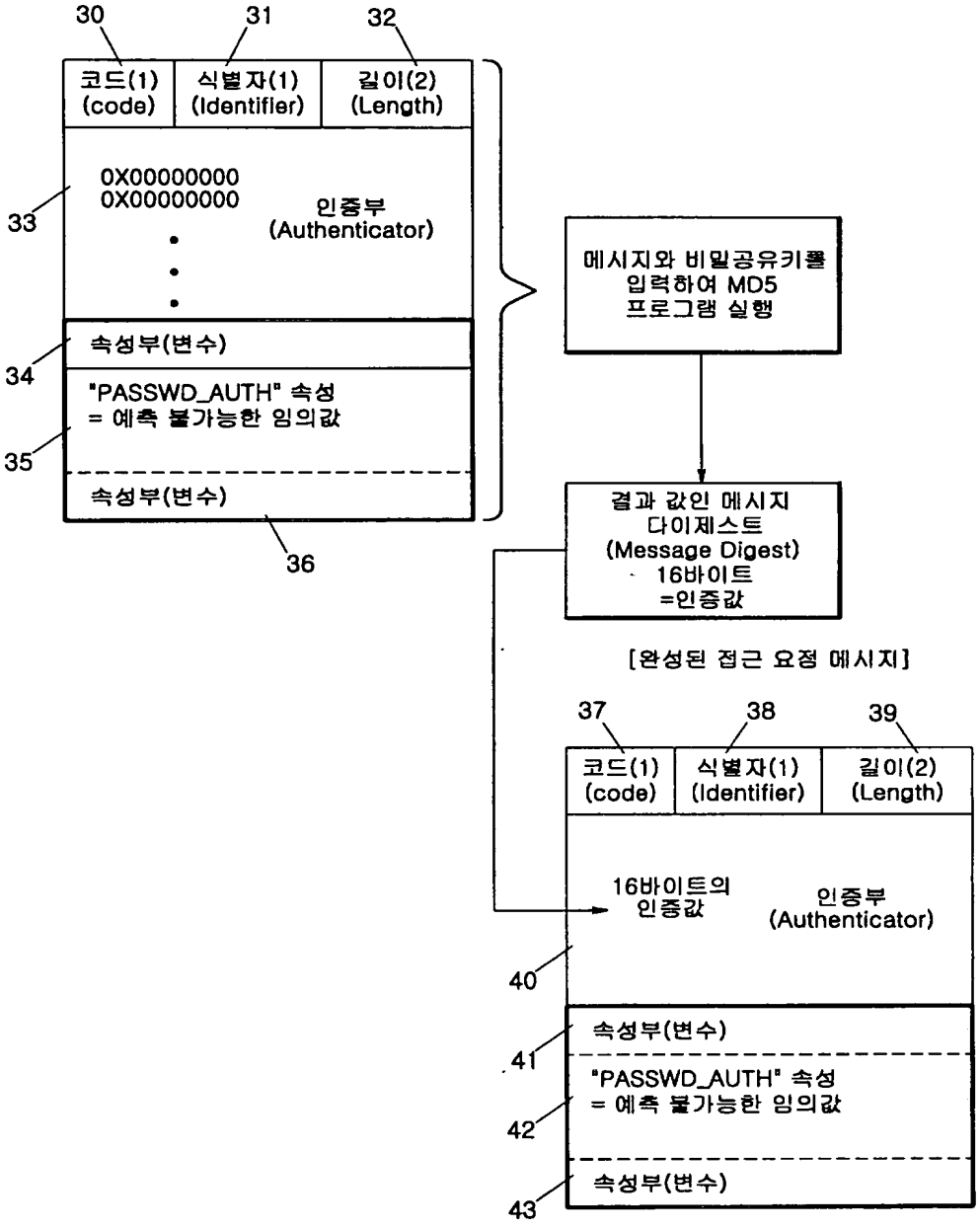
【도 1】


10
11
FA
AAA
12
접근 요청(Access-Request)
13
접근 허가(Access-Accept)
14
계정과금 요청(Account-Request)
15
계정과금 허가(Account-Response)

【도 2】


20
21
22
코드(1)
(code)
식별자(1)
(Identifier)
길이(Length) (2)
인증부(Authenticator) (16)
23
속성부(Attribute)
24

【도 3】


30
31
32
코드(1)
(code)
식별자(1)
(Identifier)
길이(2)
(Length)
0X00000000
0X00000000
인증부
(Authenticator)
33
속성부(변수)
"PASSWD_AUTH" 속성
= 예측 불가능한 임의값
34
35
속성부(변수)
36
메시지와 비밀공유키를
입력하여 MD5
프로그램 실행
결과 값인 메시지
다이제스트
(Message Digest)
16바이트
=인증값
[완성된 접근 요정 메시지]
37
38
39
코드(1)
(code)
식별자(1)
(Identifier)
길이(2)
(Length)
16바이트의
인증값
인증부
(Authenticator)
40
속성부(변수)
41
"PASSWD_AUTH" 속성
= 예측 불가능한 임의값
42
속성부(변수)
43